CLCS Mission Support Networks

CMSN Home Page

CMSN Drawing Table

Software Security Model

Security Plan

Support Servers

CMSN Glossary

The CLCS Mission Support Networks is the set of networks that provide connectivity between the CLCS Operational Control Rooms (OCR), the Business and Information workstations, the Shuttle Data Center (SDC), the Record & Playback Subsystem (RPS), CLCS Software Development and validation sets and external networks.

The CMSN will provide a centralized network management, security monitoring of the networks, network support servers and network response help desk functions.

Next Page

E-mail

Glenn.Seaton@ksc.nasa.gov

Phone: 861-7392

Fax: 861-7470

Updated: April 2, 1998

CMSN

Introduction (Cont.)

CMSN Home Page

CMSN Drawing Table

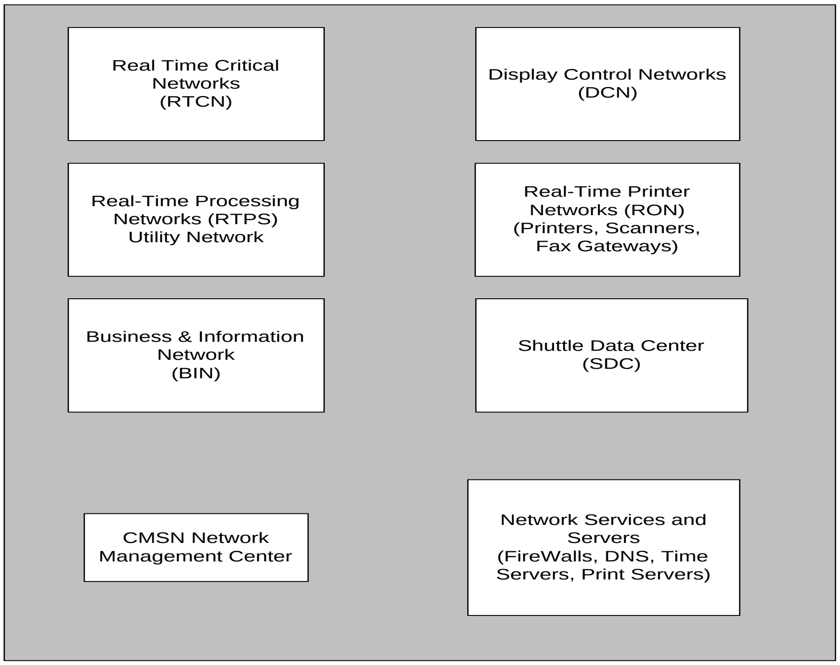
Software Security Model

Security Plan

Support Servers

CMSN Glossary

CLCS Mission Support Networks (CMSN)



Real Time Critical Networks (RTCN)

Display Control Networks (DCN)

Real-Time Processing Networks (RTPS) Utility Network

Real-Time Printer Networks (RON) (Printers, Scanners, Fax Gateways)

Business & Information Network (BIN)

Shuttle Data Center (SDC)

CMSN Network Management Center

Network Services and Servers (FireWalls, DNS, Time Servers, Print Servers)

CMSN Represents the collection of all the subsystem network componets of CLCS.
Each Subsystem has shared and independant Network Design and Management.
The overall CMSN will share common Network Management and Support Services.

E-mail Glenn.Seaton@ksc.nasa.gov

CMSN Security Plan

CMSN Home Page

CMSN Drawing Table

Software Security Model

Security Plan

Support Servers

CMSN Glossary

The objectives of the CMSN Security Plan are:

- Allow access to resources for normal Shuttle Processing without burdening users with multiple accounts and passwords.
- To provide the highest level of security short of physical disconnection of the Operational Control Room Networks.
- To meet the highest availability and reliability needed for Shuttle Processing.

CMSN Security will be based on network accessibility as well as workstation security. Specialized network equipment and network routers will provide network connectivity for operational and support systems while allowing for the highest possible security mandated for each system security level. Network security will be established by utilizing staged firewalls, routers, gateways and network monitors.

Network security measures will include IP packet filtering, real-time session monitors, network firewalls providing protocol filtering, proxy servers and Network Address Translation technology. Supporting the real-time monitoring will be network logs of network sessions for post event analysis, utilization trends and network bottleneck identification.

Firewalls will separate the areas with differing levels of security requirements. With the exception of specialized traffic types and flows, all traffic between security levels will flow through a firewall. The firewalls between each level will be of differing vendors and firewall types to better isolate product weaknesses, bugs in hardware or software, reducing potential breeches of security. This prevents the entirety of CMSN from being exposed by one exploit technique or bug.

Security restrictions for workstations in the RTPS will be part of the security plan. Those workstations will be able to establish network sessions to other CMSN systems. No EMAIL, X-Windows or other network processes will be permitted from RTPS systems to External CMSN locations. World Wide WEB access for CMSN will be filtered by a proxy WEB server such as provided by the LPSWEB server.

Configured workstation on the BIN will have less restrictive access control than RTPS Command and Control Workstations, but will have automated configuration management. Laptops and other portables allowed on the BIN will be network managed and monitored from the Network Control Center.

Security Model

Updated: April 2, 1998

E-mail

Glenn.Seaton@ksc.nasa.gov

Drawing Table

This is the master index to the CLCS Mission Support Networks Drawings.

CMSN Home Page

CMSN Drawing Table

Software Security Model

Security Plan

Support Servers

CMSN Glossary

CMSN Support Network Drawings List

- CMSN Master Connectivity
- Security Model
- Typical RTPS layout
- Typical BIN Layout

E-mail Glenn.Seaton@ksc.nasa.gov

CLCS Software Development Model

CMSN Home Page

CMSN Drawing Table

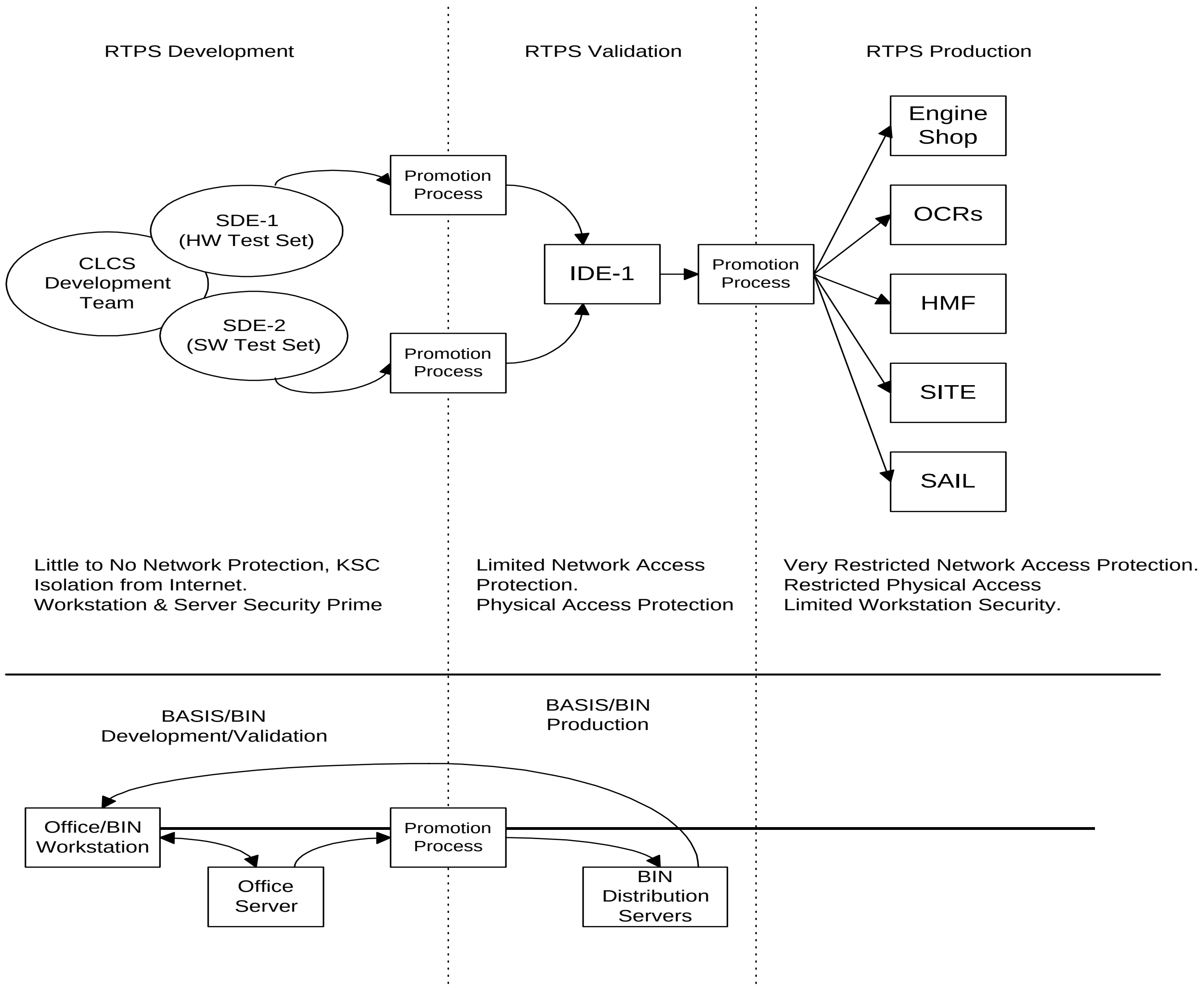
Software Security Model

Security Plan

Support Servers

CMSN Glossary

CLCS Network Security Software Development & Promotion Process Concept



RTPS Development

RTPS Validation

RTPS Production

Little to No Network Protection, KSC Isolation from Internet.
Workstation & Server Security Prime

Limited Network Access Protection.
Physical Access Protection

Very Restricted Network Access Protection.
Restricted Physical Access
Limited Workstation Security.

BASIS/BIN Development/Validation

BASIS/BIN Production

E-mail Glenn.Seaton@ksc.nasa.gov

CMSN Home Page

CMSN Drawing Table

Software Security Model

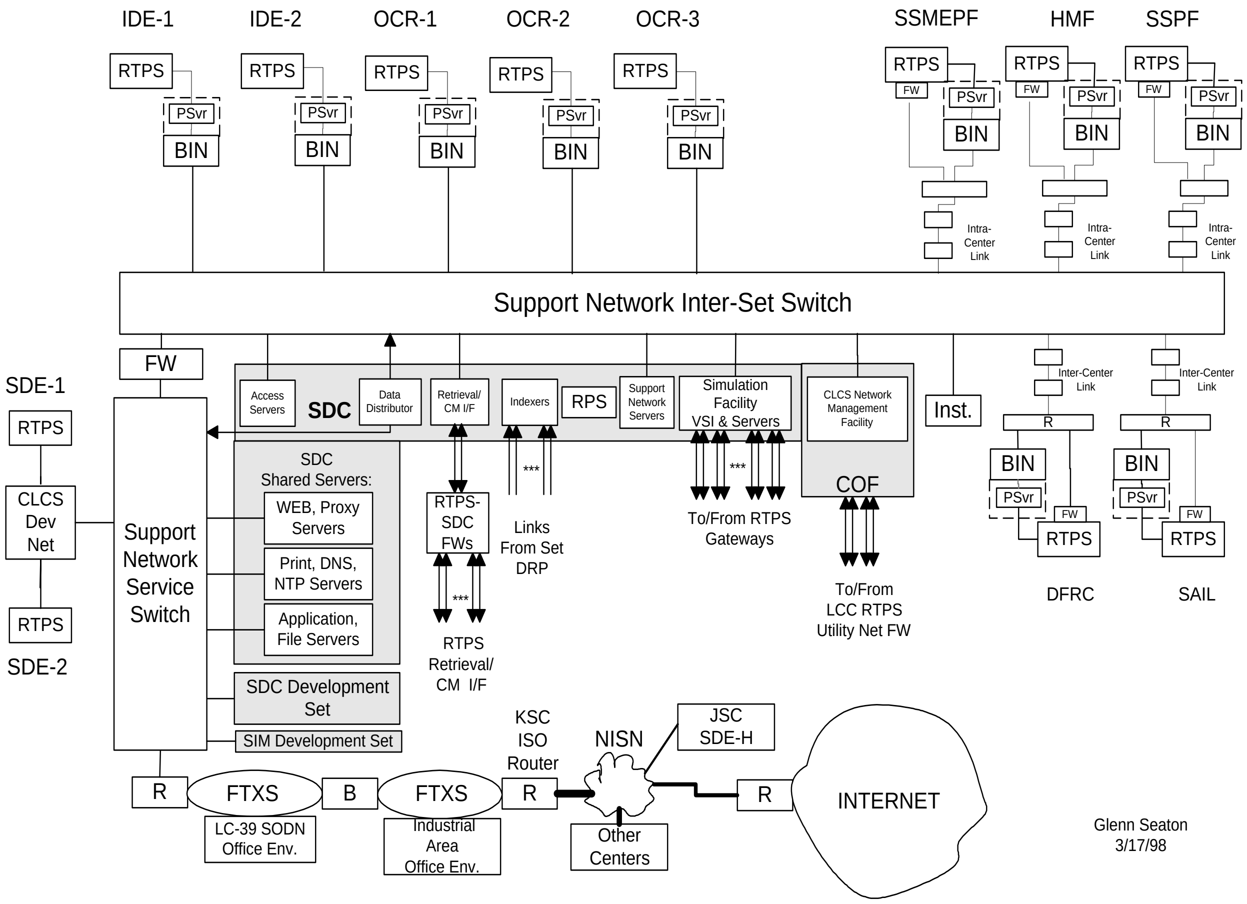
Security Plan

Support Servers

_CMSN Glossary

Previous Page Next page

CLCS Mission Support Network
Architectural End Game



Glenn Seaton
3/17/98

Updated : 2 April, 1998

CMSN Home Page

CMSN Drawing Table

Software Security Model

Security Plan

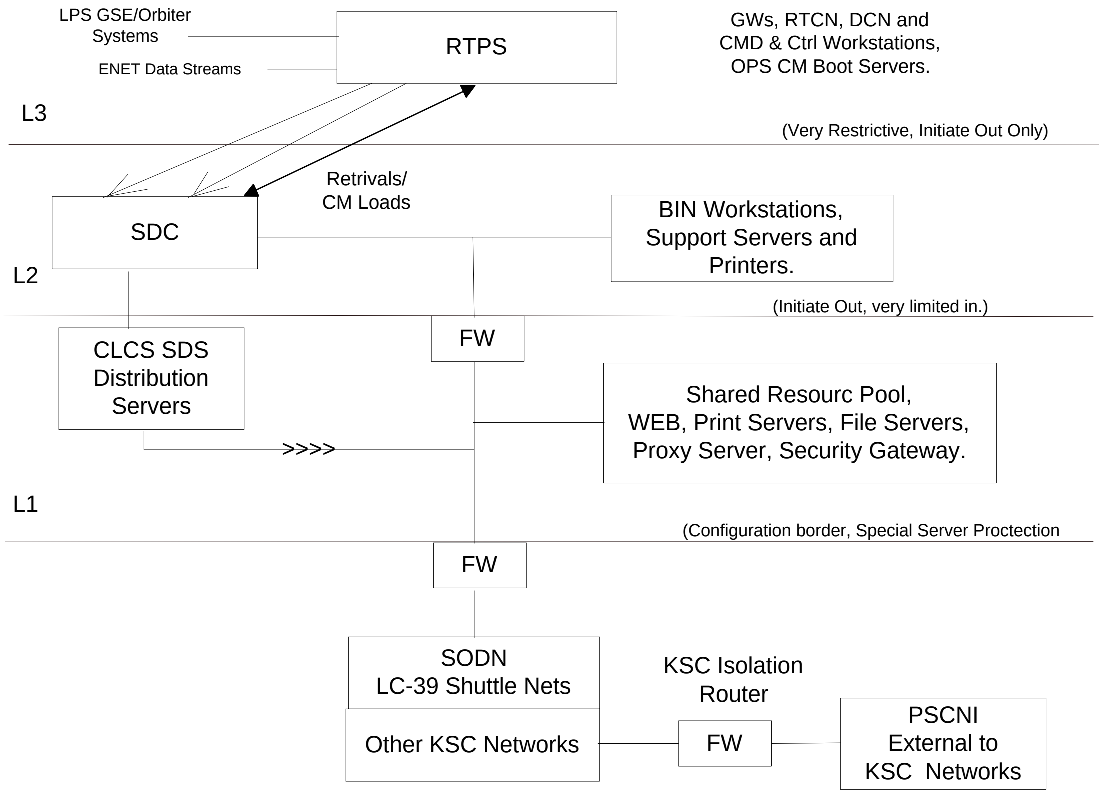
Support Servers

_CMSN Glossary

Previous Page Next page

CLCS Mission Support Networks (CMSN)

Network Security Concept


LPS GSE/Orbiter Systems
ENET Data Streams
RTPS
GWs, RTCN, DCN and CMD & Ctrl Workstations, OPS CM Boot Servers.
L3
(Very Restrictive, Initiate Out Only)
Retrivals/ CM Loads
SDC
BIN Workstations, Support Servers and Printers.
L2
(Initiate Out, very limited in.)
FW
CLCS SDS Distribution Servers
>>>>
Shared Resourc Pool, WEB, Print Servers, File Servers, Proxy Server, Security Gateway.
L1
(Configuration border, Special Server Proctection
FW
SODN LC-39 Shuttle Nets
Other KSC Networks
KSC Isolation Router
FW
PSCNI External to KSC Networks

Glenn Seaton
DE-CLC
1-7392

Updated : 2 April, 1998

CMSN Home Page

CMSN Drawing Table

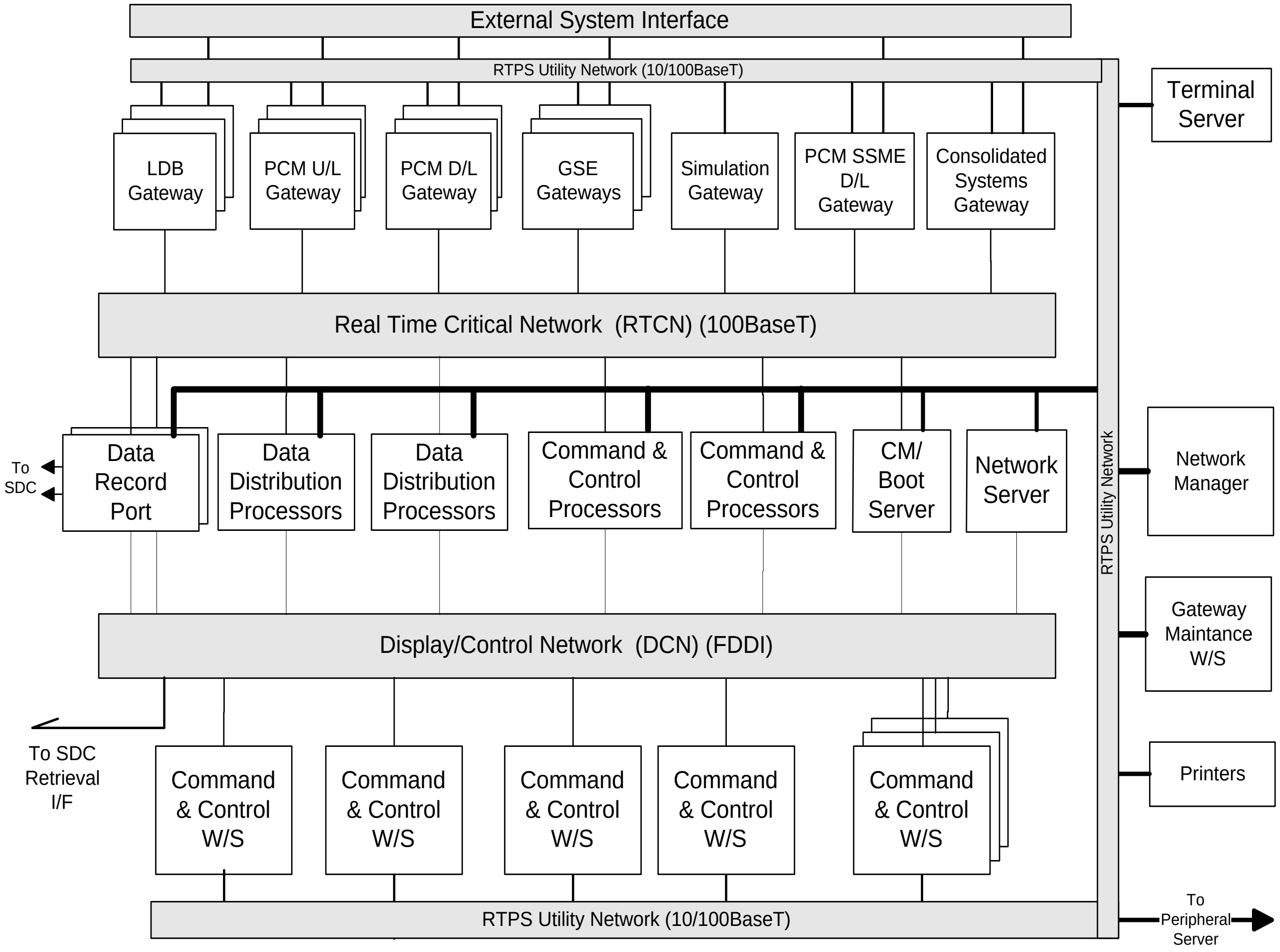
Software Security Model

Security Plan

Support Servers

_CMSN Glossary

Previous Page Next page

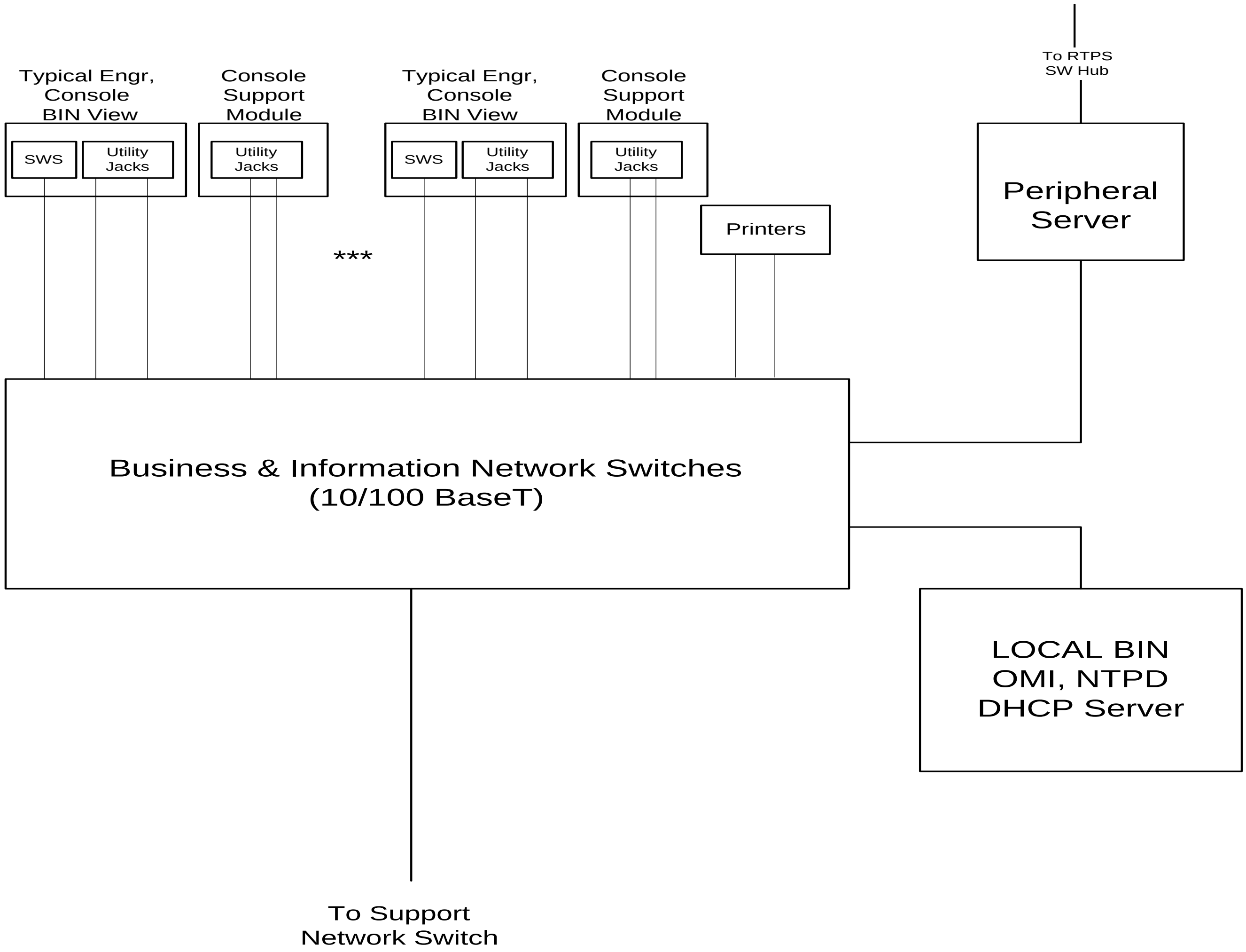


Real-Time Processing System
Test Set

Updated : 2 April, 1998

Previous Page Next page

Business and Information Support Set



Updated : 2 April, 1998

CMSN Support System Servers

Previous Page   Next page

OMI Server
The OMI Server is a local BIN server designed to provide rapid response to on-line OMI documentation and Goody Book type information. The physical server is located on the BIN Support network to limit access to the local BIN users. The OMI Server is a WEB based process and will provide mirrored documentation from sources on the LPSWEB master WEB server. The OMI Server will also provide NT Domain registration, local Configuration Management using Microsoft SMS if BIN workstation are NT base workstations. It will also provide the Network Time Server function and backup print server for the BIN.

Peripheral Server
The Peripheral Server provides shared Print Services, Fax machines and Scanners to RTPS and BIN users. The printers will be network devices accessed via the Utility Network or BIN via the Peripheral Server or the individual sub-system needing access to the printer. The Peripheral Server provides the connection between the users and the shared printers, faxes and scanners physically connected to the RTPS and BIN network loops. To support network security issues, it will not provide any additional functions, will not provide file sharing or support remote administration.

RTPS Firewall
The RTPS Firewall will provide network security between the Level 2 security of the BIN and the Level 3 security support of the RTPS. It will allow RTPS network access out of the RTPS to targeted systems and reply messages but will not support external systems access to RTPS systems.   It will connect the external Level 2 Network Switch to the RTPS Utility network. The only supported protocols will be TCP/IP. RTPS systems will be provided with private network addresses using network IP 10.a.b.c.   Where 10.a will identify a Flow Zone, b will identify network group and c the individual system.

Network Switch Firewall
The Firewall that interfaces the Level 1 Support FDDI ring and the Network Switch will be used to interface the Level 1 to the Level 2 Network Switch interset connector. The protocols that will be allowed are IP based TCP and UDP sub-protocols.
It will allow internal workstations and servers to connect to external systems. Normal reply messages will be allowed and limited special traffic such as X traffic. The Smart Card Gate will allow inbound network connections after user has passed the User Id, User Personal Identification Number and Smart card ID to BIN Workstations and Servers on the Level 2 network.

Next page

CMSN Home Page

CMSN Drawing Table

Software Security Model

Security Plan

Support Servers

_CMSN Glossary

CMSN Support System Servers

Previous Page Next page

External Firewall
The Firewall used to interface the CLCS Support FDDI ring to KSC and External center networks. It will provide a Security Level 0 to Level 1 transition. Servers on the Global Support ring are intended to provide support for both internal and external users. The Support Ring is provides the connection for the Shuttle Data Center external users to do data retrievals.

RTPS Utility Network Manager
The RTPS Utility Network Manager will provide network SNMP management of all the devices on the Utility Network and report local status for the state of the RTPS Utility Network and report events and alarms to the External Master CLCS Network Management Station.

CLCS Net Manager
The CLCS Network Manager will be a master Network Manager that will configure, monitor and manage the CLCS Support Network infrastructure and receive Network event messages from the remote RTPS Network Management stations.

Smart Card Gateway
To support access to secure network system from an less secure network, a hardware and software Smart Card Gateway provides electronic badge checking and user authentication using a constantly changing password key as part of the user password. User connects to the Smart Card Gateway, enters a User Id and a password based on an individual identification number combined with a code provided by there Smart Card. The server then allows validated users access to a secure system.

Proxy Server
The Proxy Server is a applications running on a WEB Server, such as LPSWEB, that WEB browsers connect to, to access the WEB. For CLCS operational areas it will limit what WEB sites can be accessed, the default is the *.GOV domain. The workstations that are accessing the WEB via the proxy are not visible to the WEB site being accessed. The proxy relays the request to the remote site and provides its network address as the return path., then forwards the response back the the requesting workstation.

CMSN Support System Servers

Previous Page Next page

Domain Name Server
While KSC has several Network Domain Name servers, servers that translate network names such as a WEB browser URL, to the actual network address. CLCS will have one on the primary network switch to improve response and availability. It will be a caching type server meaning it will keep copies of addresses requested often and forward request to external Domain Name Servers for address it does not know.

NTPD Server
The Network Time Protocol Server Deamon is a application running on a server that provides time to network devices. It uses the Network Time Protocol to distribute time and to request time from a Network Time Master Server. The Network Time Protocol uses several message to calibrate the time delta between the sender and the receiver.

Intra Facility Router
To support multiple network addresses connected to the same network segment as planned to support the BIN workstations using DHCP, a Intra Facility Router is needed. This router tells the workstations on the same segment how to get to printers and servers on the same segment that have different network address ranges. The main requirement for this router is to reduce the network traffic from the firewall router for internal messages.

Private Subnet distribution (192.168.0.0)

CMSN Home Page

CMSN Drawing Table

Event CalendarSoftware

Security Plan

Support Servers

_CMSN Glossary

Glossary of CLCS Network Terms

Previous Page Next page

ATM - Asynchronous Mode Transfer - 155 Mbs (OC-3) packetized data

BIN - Business Information Network: Provides network communications between external data sources and the HCI subsystems.

BASIS - Business and Support Information Service: The application suite and tools to provide information for CLCS users on the BIN and in their office enviorment.

CCP - Command and Control Processing: Processes Gateway data and presents it to the HCI. Dual homed to both the RTCN and the DCN.

CCWS - Command & Control Workstation (was HCI).

CLCS - Checkout, Launch and Command Subsystem: the replacement for the LPS.

CMSN - CLCS Mission Support Networks: Includes the RTCN, RTPS utility network, BIN, DCN, RON, SDC, Network Management functions, and network servers and services.

DCN - Display and Control Network: Part of the RTPS. Provides the transmission means for communications between the HCI, DDP, and CCP subsystems.

DDP - Data Distribution Processing: Dual homed to both the RTCN and the DCN.

DRP - Data Recording Port: The interface between CLCS and SDC to transfer information to SDC from CLCS to be recorded.

DSR - Display Synchronous Rate

HCI - Human Computer Interface: the workstations for users of the RTPS.

LON - LPS Operational Network

RTCN - Real Time Critical Network: Part of the RTPS. Provides the transmission means for communications between the Gateway (FEP equivalents) subsystems, the Command and Control Processing subsystems, and the Shuttle Data Center.

RTPS - Real Time Processing System: The combined processing system including Gateways, RTCN, DCN and Cmd and Ctrl Workstations, and OPS CM Boot Server.

SODN - Shuttle Operations Data Network

SSR - System Synchronous Rate: Measurement change data from the Gateways is transferred on the RTCN relative to this. RTPS system software establishes a staggered start time from the SSR for each Gateway subsystem. Command data is asynchronous.

NISN - NASA Intra-Center Service Network

DHCP - Dynamic Host Configuration protocol